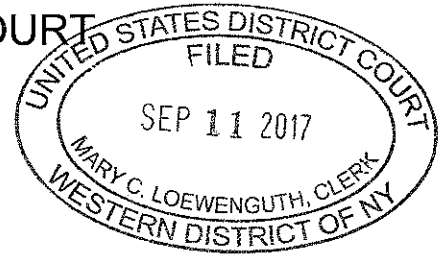


UNITED STATES DISTRICT COURT

for the
Western District of New York



In the Matter of the Search of
(Briefly describe the property to be searched or identify
the person by name and address.)

Case No. 17-MJ- 636

IN THE MATTER OF THE SEARCH OF:

Google Inc. Gmail ("Google") account
"woolyacresfarms@gmail.com,"
("woolyacresfarms") and
"countryboy999999@gmail.com"
("countryboy999999")

APPLICATION FOR A SEARCH WARRANT

I, NIKKI TOLIAS, a Federal Law Enforcement Officer, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Western District of New York (identify the person or describe property to be searched and give its location):

The subject property to be searched: Google Inc. Gmail ("Google") account "woolyacresfarms@gmail.com," ("woolyacresfarms") and "countryboy999999@gmail.com" ("countryboy999999"), as described in Attachment A.


The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized): **See Attachment B for the Items to be Seized, all of which are fruits, evidence and instrumentalities related to a violation of Title 18, United States Code, Section 2252A(a)(5)(B), all of which are more fully described in the application and affidavit filed in support of this warrant, the allegations of which are adopted and incorporated by reference as if fully set forth herein.**

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of **Title 18, United States Code, Section 2252A(a)(5)(B)**, and the application is based on these facts which are continued on the attached sheet.

☐ Delayed notice of 90 days is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

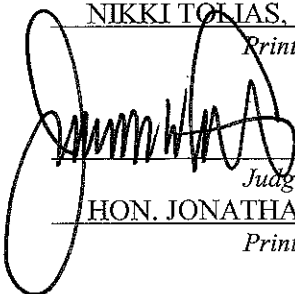
NIKKI TOLIAS, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: September 11 2017

City and State: Rochester, New York


Judge's signature

HON. JONATHAN W. FELDMAN, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A - GOOGLE

Property to be Searched

This warrant applies to information associated with the following email accounts stored at premises owned, maintained, controlled, or operated by Google, Inc., a company located at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

- a. woolyacresfarms@gmail.com
- b. countryboy999999@gmail.com

ATTACHMENT B - GOOGLE

Information to be Seized

Because Google, Inc. (Google) is not aware of the facts of this investigation, its employees are not in a position to search for relevant evidence. In addition, requiring Google to perform the search would be a burden upon the company. If all Google is asked to do is produce all the files associated with the account, an employee can do that easily. Requiring Google to search the materials to determine what content is relevant would add to their burden. Therefore, in order to ensure that agents search only those computer accounts and/or computer files described herein, this search warrant seeks authorization to permit employees of Google, to assist agents in the execution of this warrant. To further ensure that agents executing this warrant search only those accounts and/or computer files described below, the following procedures have been implemented:

1. The warrant will be presented to Google, personnel by law enforcement agents. Google, personnel will be directed to isolate those accounts and files described below;
2. In order to minimize any disruption of computer service to innocent third parties, the system administrator will create an exact duplicate of the accounts and files described in Attachment A, including an exact duplicate of all information stored in the computer accounts and/or files described below;
3. The Google, system administrator will provide the exact duplicate of the accounts and files described below and all information stored in those accounts and /or files to the Special Agent who serves this search warrant;

4. Law enforcement personnel will thereafter review the information stored in the accounts and files received from the system administrator and then identify and copy the information contained in those accounts and files which are authorized to be further copied by this search warrant;

5. Law enforcement personnel will then seal the original duplicate of the accounts and files received from the system administrator and will not further review the original duplicate absent an order of the Court.

I. Information to be disclosed by Google

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Google, is required to disclose the following information to the government for each account or identifier listed in Attachment A from May 30, 2016 to August 10, 2016:

a. The contents of all e-mails stored in the account, including copies of e-mails sent to and from the account, draft e-mails, attachments, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail.

b. Any deleted emails, including information described in subparagraph "a," above.

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number).

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files

e. All records pertaining to communications between Google and any person

regarding the account, including contacts with support services and records of actions taken.

f. Any documents, folders, folder names and directory listing, images, data, videos and attachments stored within this account or accessible by users woolyacresfarms and countryboy999999. This would also include images, data, videos, documents, and attachments stored in Google cloud storage, bucket storage, Google+, Google drive, Picasa, Google Dashboard, and any other online storage accessible by users woolyacresfarms and countryboy999999.

g. All date, time and IP Addresses for each uploaded and download file as well as all Share settings for Google cloud storage, bucket storage, Google+, Google drive, Picasa, Google Dashboard, and any other online storage accessible by Google users woolyacresfarms and countryboy999999.

h. All previously preserved data in the account to include what is detailed in paragraphs a-g above.

II. Information to be seized by the government

All records or information, including the contents of any and all electronic communications, attachments, stored files, print outs, and header information that contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(5)(B), (Possession of Child Pornography) (for each account or identifier listed on Attachment A, such information to include:

- a. The contents of any such communications that will assist investigators in ascertaining the nature and scope of the crimes under investigation, the true identity and or location of the subjects and any co-conspirators, the names, addresses, sources of the child pornography;
- b. Records relating to who created, used, or communicated with the account or identifier;
- c. Records, including, but not limited to, video files, audio files, images, stored messages, recordings, books, documents, and cached web pages relating to child pornography;
- d. Deleted files that may have contained images of child pornography;
- e. Records reflecting the communications with or the existence, identity, travel, or whereabouts of any co-conspirators;
- f. Any other identifying information associated with the user of the account (financial information, employment information, patterns of behavior, etc.).

ADDENDUM TO SEARCH WARRANT
SEARCH OF COMPUTERS

1. The computer or electronic media search authorized by this warrant shall be completed within 60 days from the date of the warrant unless, for good cause demonstrated, such date is extended by Order of this Court.

2. In conducting the search authorized by this warrant, the government shall make reasonable efforts to utilize computer search methodology to search only for files, documents or other electronically stored information which are identified in the warrant itself.

3. Should the government not locate any of the items specified in the warrant (or other fruits, contraband, instrumentalities, or property subject to forfeiture) within the authorized search period (including any extensions granted), the government shall return the computer or electronic media to the owner.

4. In any circumstance not covered by paragraph three (3) above, upon completion of the search, the government, upon request of the owner of the computer, shall promptly return to the owner of the computer copies of all files and documents requested and specified by the owner, excluding any items or files seized pursuant to the warrant or other fruits, contraband, instrumentalities or property subject to forfeiture.

5. If electronically stored data or documents have been identified by the government pursuant to this warrant, or other fruits, contraband, instrumentalities or property subject to forfeiture, the government may retain the original hard drive or other data storage mechanism pending further order of this Court. The retention of the original hard drive or other data storage mechanism does not relieve the government of its obligation to return to the owner of the computer files, documents or other electronically stored information identified in paragraph (4) above.

6. Nothing in this warrant shall limit or prevent the government from retaining the computer or electronic media as fruits, contraband or an instrumentality of a crime or commencing forfeiture proceedings against the computer and/or the data contained therein. Nothing in this warrant shall limit or prevent the owner of the computer or electronic media from (a) filing a motion with the Court pursuant to Rule 41(g) of the Federal Rules of Criminal Procedure for the Return of Property or (b) making a request of the government to return certain specified files, data, software or hardware.

7. Should there be a dispute or question over ownership of any computer or any electronically stored data or documents stored therein, the government shall promptly notify this Court so that such dispute or question can be resolved.

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

STATE OF NEW YORK)
COUNTY OF MONROE) SS:
CITY OF ROCHESTER)

I, NIKKI TOLIAS, being duly sworn, depose and state the following:

1. I am a Special Agent with Homeland Security Investigations (HSI) within the Department of Homeland Security, assigned to the office of the Special Agent in Charge, Buffalo New York, and have been so employed since 2006. Before that, I was employed by the former Immigration and Naturalization Service (INS) for approximately nine years. As part of my duties as a Special Agent with HSI, I investigate criminal violations relating to child exploitation and child pornography, including the illegal distribution, receipt and possession of child pornography, in violation of Title 18, United States Code, Sections 2252 and 2252A. I have received specialized training in the area of child pornography and child exploitation, and I have had the opportunity to observe and review numerous examples of child pornography, as defined in Title 18 United States Code, Section 2256.

2. As set forth in more detail below, there is probable cause to believe that evidence, contraband, fruits and instrumentalities of violations of Title 18, United States Code, Section 2252A (receipt and possession of child pornography) are contained within Google account. These items are more specifically described in Attachment B.

3. The statements contained in this affidavit are based upon my investigation, information provided to me by other law enforcement personnel, and on my experience and training as a Special Agent of HSI. Because this affidavit is being submitted for the limited purpose of establishing probable cause to secure a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Section 2252A.

4. I make this affidavit in support of an application for a search warrant for the Google Inc. Gmail ("Google") account "woolyacresfarms@gmail.com," ("woolyacresfarms") and "countryboy999999@gmail.com" ("countryboy999999"). The e-mail service provider, Google, is located at 1600 Amphitheatre Parkway, Mountain View, California, and controls this account.

5. The information set forth in this affidavit is provided for the sole purpose of establishing probable cause for the issuance of the search warrant; therefore, does not necessarily contain all facts uncovered during this investigation.

6. Pursuant to the provisions of Title 18, United States Code, section 2252A(a)(5)(B), it is a federal crime for any person to knowingly possess child pornography and knowingly accessed with intent to view, any material that contains images of child pornography that have been mailed or, using any means or facility of interstate or foreign

commerce, have been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer and that the images were produced using materials that have been mailed, shipped or transported in or affecting interstate of foreign commerce by any means including computer.

7. Pursuant to Title 18, United States Code, Section 2703(b), the contents of an electronic communication that is in electronic storage in an electronic communications system for more than 180 days may be obtained “pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with *jurisdiction over the offense under investigation...*” (emphasis added). Further, pursuant to Title 18, United States Code, Section 2703(b)(1)(A), where such a warrant is obtained, no notice to the subscriber or customer is required to be given.

TRAINING AND EXPERIENCE

8. Based on my training and experience, including conversations with representatives from Google and with other law enforcement officers, I have learned the following about Google:

- a. Google provides a variety of on-line services, including electronic mail (“e-mail”) access, to the general public. Google allows subscribers to obtain e-mail accounts at the domain name “googlemail.com”, or “gmail.com” like

the email account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and un-retrieved e-mail for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, e-mail transaction information, and account application information.

b. In general, an e-mail that is sent to a Google subscriber is stored in the subscriber's "in-box" on Google servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Google servers indefinitely. The user can move and store messages in personal folders such as a "sent folder." In recent years, Google and other Internet Service Providers ("ISPs") have provided their users with larger storage capabilities associated with the user's email account. Google and other ISPs have allowed users to store up to ten (10) gigabytes of information associated with the account on ISP servers. Based on conversations with other law enforcement officers with experience in executing and reviewing search warrants of email accounts, I have learned that search warrants for email accounts and computer systems have revealed stored emails sent and/or received many years prior to the date of the search.

c. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Google's servers, and then transmitted to its end destination. Google often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Google server, the e-mail can remain on the system indefinitely.

d. A sent or received e-mail typically includes the content of the message, source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by Google but may not include all of these categories of data.

e. A Google subscriber can also store files, including e-mails, address books, contact or buddy lists, calendar data, pictures, and other files on servers maintained and/or owned by Google. Subscribers to Google might not store, on their home computers, copies of the e-mails stored in the Google account. This is particularly true when they access their Google account through the web, or if they do not wish to maintain particular e-mails or files in their residence.

f. In general, e-mail providers like Google ask each of their subscribers to provide certain personal identifying information when registering for an e-

mail account. This information could include the subscriber's full name, physical address, telephone numbers and other identifiers, such as alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

g. E-mail providers typically retain certain transaction information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol (IP) address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

h. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers

typically retain records about such communications, including records of contacts between the user and the providers support services, as well as records of any actions taken by the provider or user as a result of the communications.

i. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

j. Google users have access to various Google services that can be used to store various types of data (further described in Attachment B) such as Google Drive, Google+, Google Cloud, Google Dashboard and Picasa.

k. As set forth below, there is probable cause to believe that evidence relating to one or more criminal violations of 18 U.S.C. 2252A(a)(5)(B) is currently located within the Google Inc. Gmail account, wooleyacresfarms@gmail.com, __countryboy999999@gmail.com, and user wooleyacresfarms and countryboy999999's Google account.

PROBABLE CAUSE TO SEARCH THE EMAIL ACCOUNTS

9. On March 6, 2017, HSI Attache Brussels, Belgium received information from the Belgian Federal Police (BFP) regarding individuals in the United States that they identified during a Belgian investigation into the possession and distribution of child pornography by a Belgian citizen. In an interview with the BFP, the aforementioned Belgium subject mentioned an individual by the name of Bob who had transferred money on several occasions in exchange for child pornography. He stated that Bob was probably from the United States.

10. Information received from Paypal revealed seven payments by woolyacresfarms (email: woolyacresfarms@gmail.com) between May 30, 2016 and August 10, 2016 for a total amount of \$335.00 U.S. dollars. The investigation showed that the Belgian suspect used a Yandex email address exclusively for child pornography. The suspect gave the BFP permission to log into his Yandex email account. The BFP provided HSI with a screen shot of this account. In the Yandex inbox of their suspect there was an email from bryan scott in which the first line of the email was visible and read: "money is sent 8-10-16 hey phil just thought I would send you the money so u can send files when u get home this time for my videos very young solo or girl." A forensic exam of the Belgium subject's electronic media by the BFP revealed a folder named Bryan. It was created on May 22, 2016 and contained approximately 73 files, most of which were video files.

11. The Belgium subject was asked about several contacts he received emails from. He was questioned about the email contryboy999999@gmail.com, to which he stated was the American he mentioned previously saying that the email account users name was Bob or Robert, a typical American name. In the contacts, the name Bryan Scott was found as being linked to the email address countryboy999999@gmail.com.

12. The Paypal account of the Belgium subject was linked with the name Phil Oldham with email address phil.oldham@yandex.com. The above-referenced seven PayPal transactions were made to Phil Oldham at Phil.oldham@yandex.com by woolyacresfarms@gmail.com.

13. Open source checks indicate that the Woolyacresfarms@gmail.com email address is associated with a farm located at 8513 Creek Road, Nunda, New York. Checks of the New York State Sex Offender Registry revealed that Bryan Scott MATACALE (a registered sex offender) is residing at 8527 Creek Road, Nunda, New York.

14. Law enforcement checks indicate that Bryan S. MATACALE, date of birth: 04/13/1975 was convicted in Livingston County of Possessing an Obscene Sexual Performance by a Child in 2005 and also convicted in Steuben County of Attempted Rape 3rd, Endangering the Welfare of a Child in 2009. Bryan S. MATACALE is a registered Level 2 sex offender in New York State. Information received from the sex offender registry

indicated that MATACALE's last known address is 8527 Creek Road, Nunda, New York 14517.

15. On March 21, 2017, HSI Buffalo sent a Customs Summons to Paypal requesting subscriber information for the following:

PayPal Usernames: woolyacresfarms@gmail.com
Countryboy999999@gmail.com

Customer Name: Bryan Scott MATACALE

Addresses: 8513 Creek Road, Nunda, NY 14517
8527 Creek Road, Nunda, NY 14517

Dates requested: May 20, 2016 to March 21, 2017

On March 30, 2017, HSI Buffalo received the summons return from Paypal in response to the above listed request. There were 7 payments between May 30, 2016, and August 10, 2016 from woolyacresfarms@gmail.com in the total of approximately \$335.00 made to Phil Oldham, Phil.oldham@yandex.com.

16. In June of 2017 HSI Brussels forwarded the content of the files that were located on the Belgian Suspect's hard drive in the folder named "Bryan" which contained suspected child pornography to HSI Buffalo since they believe the folder "Bryan" is linked to Bryan Scott MATACALE who is located within HSI Buffalo's area of responsibility.

17. The undersigned viewed the suspect videos that were obtained from the suspect in Belgium's electronic media. Approximately fifteen (15) videos appear to depict children under the age of eighteen engaged in sexually explicit conduct.

18. Your Affiant has provided three examples of the material contained in this account:

- a) **"Webcam Omegle PTHC 2015 Sister Brother lick suck + dog GREAT!!!.avi"**: an video file depicting what appears to be an unclothed minor male child with an erect penis lying on a bed while a dog licks his penis. There is also what appears to be a clothed minor female sitting on the bed in front of the minor male child. The female child lifts up her shirt and bra exposing her breasts.
- b) **"!! Tara 8yo Full_001__pthc_hussyfan_kingpass_liluplanet.avi"**: a video file depicting what appears to be an unclothed prepubescent minor female child lying on top of an adult male being anally penetrated by an adult male's erect penis. During the video the same minor child is depicted giving oral sex on an adult male and also being anally penetrated by a plastic implement.
- c) **"-1.wmv"**: a video file depicting what appears to be an unclothed prepubescent female child lying down being vaginally penetrated by an adult male's erect penis.

19. On July 26, 2017, your affiant received information from New York State Police Investigator Brian Mayhew. Investigator Mayhew advised that he received a complaint in June of 2017 in which a couple in Bath, New York made an allegation that MATACALE had sexually assaulted one of their children. Investigator Mayhew initiated an investigation of MATACALE related to the allegation of engaging in sexual acts with a minor. Investigator Mayhew confirmed that the minor victim was forensically interviewed. He further advised that due to the limited disclosure of the minor victim, the invoked right to counsel of MATACALE, lack of admission by MATACALE and lack of physical evidence in the case, it was determined that there would be not sufficient information or evidence for criminal prosecution at the time.

20. On August 1, 2017, HSI Buffalo sent a summons to Hughes Net, a satellite internet company requesting subscriber information for 8527 Creek Road, Nunda, New York 14517. On August 3, 2017, Hughes Net responded with the following subscriber information:

Account Holder: Bryan Matacle

Phone: 585-519-5436

Account Number: DSS10080889

Date Established: 12/31/2012

Physical Location: 8527 Creek Road, Nunda, NY 14517

Current Site Type: Jupiter

Status: Active

Bank Number: 022000046

Bank Account Number: xxxxxx4472

Emails: Bryanmatacale@hughes.net

Woolyacresfarms@frontier.com

Woolyacresfarms@gmail.com

21. The Email account woolyacresfarms@gmail.com is linked with MATACALE's Paypal Account which was used to purchase child pornography, and that the email account countryboy999999@gmail.com was found linked to the contact "Bryan Scott" in the Belgian Suspect's email account, it is logical to conclude that:

- a. the email accounts were utilized to communicate with individuals that MATACALE traded child pornography with and/or
- b. the email accounts were utilized to receive and distribute child pornography and/or
- c. the email accounts will contain communication and or correspondence that will provide identifying information about the creator/user of this account and individuals this person traded child pornography with.

22. On August 28, 2017 HSI Buffalo Agents executed a federal search warrant at 8527 Creek Road, Nunda, New York 14517. During an interview, Bryan MATACALE stated that he had purchased child pornography via PayPal from someone overseas approximately one year ago. MATACALE told agents that he received the child pornography via his email address, countryboy999999@gmail.com.

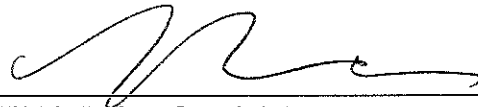
CONCLUSION

23. Based on the facts of the investigation, coupled with my training and experience as an HSI Special Agent, as well as the combined training and experience of other law enforcement officers with whom I have had discussions, Affiant asserts that the MATACALE, using Google email addresses, woolyacresfarms@gmail.com, countryboy999999@gmail.com, did knowingly possess child pornography and knowingly accessed with intent to view, any material that contains images of child pornography that have been mailed or, using any means or facility of interstate or foreign commerce, have been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer and that the images were produced using materials that have been mailed, shipped or transported in or affecting interstate or foreign commerce by any means including computer. There is probable cause to believe that additional information related to this possession is located and/or captured within the Google Inc. Gmail accounts woolyacresfarms@gmail.com and countryboy999999@gmail.com.

24. Affiant asserts that there is probable cause to believe that evidence of violations of Title 18 United States Code, Section 2252A(a)(5)(B) will be located at Google located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, within the e-mail accounts of woolyacresfarms@gmail.com and countryboy999999@gmail.com.

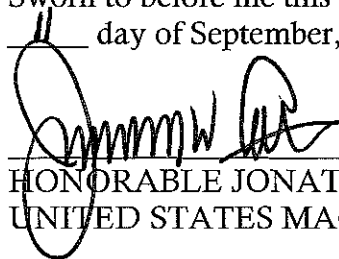
25. Wherefore by this affidavit and application, Affiant requests that the court issue a search warrant which would allow agents to search for and seize the e-mail and other information stored on the Google server for the e-mail account identified in this affidavit. Information more specifically described in Attachment B.

26. It is further respectfully requested that the Court issue an order sealing, for ninety (90) days, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the requisite inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left with the Custodian of Records at Google, Inc.). Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and premature disclosure of the contents of this Affidavit and related documents may have a negative impact on this continuing investigation and may jeopardize its effectiveness.



Nikki Tolias, Special Agent
Homeland Security Investigations

Sworn to before me this
11 day of September, 2017.



HONORABLE JONATHAN W. FELDMAN
UNITED STATES MAGISTRATE JUDGE